"Basic Endpoint Security - Compliance" Feature Overview

Endpoint Security
powered by
EGOSECURE

This document provides an overview about the "Basic Endpoint Security - Compliance" powered by EgoSecure
External Device- & Application Control

Access Control	
On cloud storage (OneDrive, GoogleDrive, Dropbox, MagentaCloud, NextCloud, OwnCloud, etc.)	✓
Anti-Bridging on LAN/ WLAN interfaces	✓
Bad USB detection / keyboard control	✓
Identify & block embedded files in Office documents (OLE)	✓
Control of audio-, video- and game controller	✓
Control of specific bluetooth functionalities (f.e. bluetooth mice and keyboards only)	✓
Control of external storages, CD/DVDs, Floppy Disk	✓
Control of digital cameras	✓
Control of local access to mobile phones (e.g. iOS, Android, MTP, PTP, Blackberry)	✓
Control of local printers	✓
Control of modems, bluetooth adapter, infrared, WiFi, ISDN adapter	✓
Control of network shares	✓
Control of smart cards	✓
Control of USB, Serial, Parallel, Firewire, PCMCIA and specific device classes	✓
Control removable media in Citrix XenApp / XenDesktop separately	✓
Control removable media in WTS separately	✓
Control of scanner and cameras	✓
Dedicated evaluations of the configurations made	✓
Detection of LAN turtles / Control of USB-Network adapter	✓
Device whitelists to the criteria of serial number, VolumeID and / or HardwareID	✓
Differentiation according to online / offline profiles	✓
Emergency button for immediate blocking of all devices (in case of safety-critical incidents)	✓
File inspection** (for example, according to IBAN pattern, credit card identifier, passport and personnel ID)	✓*
Filter of certain file formats on allowed devices (White-/Blacklist)	✓
Additional internal HDDs can be managed, logged and encrypted like external devices	✓
Grand access on individual interfaces by:	✓
Device-type	✓
Time-controlled: e.g. specific minutes, hours or days from time of activation	✓
Permit individual CD / DVD data carriers according to hash value	✓
Restrict the amount of data transfered to mass storage	✓
Whitelist of Wi-Fi Networks	✓

Secure Audit	
Monitors access to:	✓
Removable Disk	✓
CD / DVD	✓
Network directories	✓
Used WLAN hotspots	✓
Data traffic on http / https	✓
Monitoring unauthorized access	✓
Anonymized access to audit logs	✓
Protected access to user / computer information by the 4-6-eye principle	✓
Overview of the USB devices used	✓
File shadowing of data transfers via USB at the user level	✓
Monitor System Events	✓
Delivery of messages about access violations by email to administrator, etc.	✓
Monitoring of execution and usage of applications	✓
Export of revision and audit data via CSV, SNMP, SMTP (f.e. for SIEM connection)	✓

Removable Device Encryption	
Automatic (and transparent to the user) encryption of file transfer	✓
Automatic decryption of data during read operations of removable media	✓
Support of removable media and CD / DVD	✓
Decryption by Master Key	✓
Encryption/Decryption on Android devices	✓
Encryption/Decryption on iOS devices	✓
Encryption/Decryption on MacOS	✓
Different encryption types: Company Key, Group Key, Private Key	✓
Distinction between enforced encryption and selectable user-level encryption.	✓
No external CA or PKI needed	✓
Portable application for decryption by password or PKI	✓
Possibility to store differently encrypted and unencrypted files on a medium	✓
Support of TripleDES 192 and AES 256 bit encryption	✓
The disk does not need to be prepared before the first encryption	✓
Process based encryption	✓
Optional: Multi-factor-Authentication (eToken, Smart Card, Yubikey)	✓

Application Control	
Black- or Whitelisting	✓
Control applications with broken signature	✓
Demo Mode (non-blocking mode - just for warnings)	✓
DLL Control	✓
Learning-Mode	✓
Online-Offline Scenario	✓
Packages for application hash-value	✓
Scan function of application hash-value and vendor certificates	✓
Trusted Objects by vendor certificates, program path and application owner	✓
Unblocking Code	✓
Connector to Matrix42 client management	✓
Antivirus **	✓**

ADMINISTRATOR UI	
Multi-Language support for console and client component	✓
Multi-level predefined granular administrator roles and access permissions	✓
Customizable Client Messages	✓
Console layout editor	✓
Detailed reports	✓

Infrastructure, further information and system requirements	
Audit security according to Basel II, Sarbanes Oxley, PCI	✓
Export/ Import of configurations	✓
Fast user change to client component (no Windows logout needed)	✓
Intelligent push & pull or polling method for client-server communication	✓
Multi-Domain, Multi-tenancy and Managed-Services-Provider model supported	✓
Offline-support (Unblocking Code, Challenge Response, etc.)	✓
Only one management interface, one sql database, one client component needed	✓
Synchronisation of existing AD, NDS, oLDAP (read-only) and own directory	✓
Mail notifications	✓

REMARKS

Contact Matrix42 to get more information for your specific project requirements.
✓* = Add-On Deep Content Inspection
✓** = Add-On Antivirus
** = Add-On can be licensed via request to Matrix42 sales department

COMPATIBLE TO FOLLOWING OPTIONS OF MANAGEMENT SERVER CONFIGURATION

Windows 2008 R2 SP1 and higher
Separate, existing Microsoft SQL 2008 R2 /2012 and higher, Standard Edition and higher/ MySQL 5 and higher
Management Server: 64 Bit Quad Core CPU, 2.66 GHz Xeon or faster, 8 GB RAM, 80 GB disk space, 1 GB network interface card
Virtual Machine Support: VMware ESXi, Microsoft Hyper V
Customer specific design will be finalized during project implementation phase